2681

Patent
Attorney's Docket No. 032927-028

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)
	)
Ben SMEETS et al.	) Group Art Unit: 2681
	)
Application No.: 10/005,080	) Examiner: Unassigned
	)
Filed: December 7, 2001	)
	)
For: METHOD AND SYSTEM FOR	)
AUTHENTICATION OF UNITS IN A	)
COMMUNICATIONS NETWORK	)

RECEIVED

MAR 2 7 2002

Technology Center 2600

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign applications in the following foreign countries is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Danish Patent Application No. PA 2000 01844

Filed: December 8, 2000

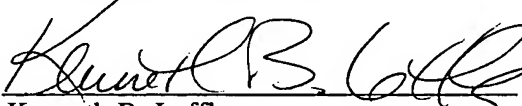European Patent Application No. EP 01610019.0

Filed: March 6, 2001

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: March 25, 2002

By: _____
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

(03/01)

Kongeriget Danmark

Patent application No.:   PA 2000 01844

Date of filing: 08 December 2000

Applicant: Telefonaktiebolaget L M Ericsson (publ)
SE-126 25 Stockholm
Sverige

This is to certify the correctness of the following information:

The attached photocopy is a true copy of the following document:

-     The specification, claims and figures as filed with the application
     on the filing date indicated above.

**Patent- og
Varemærkestyrelsen**

Erhvervsministeriet

Taastrup, 24 October 2001

Karin Schlichting
Head Clerk

Hofman-Bang

Telefonaktiebolaget L M Ericsson (publ)
SE-126 25 Stockholm
Sverige

Modtaget

- 8 DEC. 2000

PVS

Date	December 8, 2000
Your ref.	
Our ref.	P200001305 DK HSC/ASC

Method and system for authentication of units in a communications network

Method and system for authentication of units in a
communications network

----

5   This invention relates to the authentication of units in
a communications network and, more specifically, the
authentication of units in a Bluetooth network.

It is an object of the invention to provide a method and
system for fast authentication.

10   This and other objects are achieved by a method of
granting, to a user communications device, access to a
plurality of service communications devices providing a
service, the method comprising the steps of

initiating a first communications link between the user
15   communications device and a first one of the plurality of
service communications devices;

creating an access key code indicative of the user
communications device and the service;

storing the access key code in a first storage means of
20   the user communications device;

transmitting the access key code from the first service
communications device to at least a second one of the
plurality of service communications devices;

initiating a second communications link between the user
25   communications device and the second service
communications device; and

using the access key code to mutually authenticate the
user communications device and the second service
communications device.

Consequently, an access key code is generated during an initial communications session between the user communications device and one of the service communications devices. The established access key code
5   is subsequently stored in the user communications device and made available to the service communications devices. Therefore, the access code may be used in subsequent communications sessions between the user communications device and any one of the service communications devices.
10 It is an advantage of the invention that only one access key code for the service needs to be stored in the user communications device, thereby saving storage capacity in the users communications device. It is a further advantage of the invention, that a fast authentication
15 may be performed in subsequent sessions on the basis of the established access key code. It is a further advantage of the invention, that different security levels may be applied to different services.

A service according to the invention may be any service
20 provided by a service provider to a user which includes transactions between a user communications device and service communications devices. Examples of such services include the payment of tickets to e.g. public transportation, museums, concerts, etc., access control
25 and supervision of buildings, areas, etc., flexing in and out by employees, e-commerce applications, or the like.

The communications link may use any suitable communications channel, including a wireless communications link, e.g. radio-based, infrared or the
30 like.

In a preferred embodiment of the invention the communication is compliant with the Bluetooth standard.

The service communications devices may be interconnected in a network with multiple nodes. When the step of transmitting the access key code comprises the step of transmitting the access key code via a secure network connection, a secure infrastructure for the distribution of the access key codes from the first service communications device to other service communications devices is provided.

The user communications device may be part of an electronic equipment, where the term electronic equipment includes computers, such as stationary and portable PCs, stationary and portable radio communications equipment. The term portable radio communications equipment includes mobile stations such as mobile telephones, pagers, communicators, i.e. electronic organisers, smart phones, PDAs, or the like.

The first storage means may for example be a physical memory, such as a RAM, in the user communications device or a, possibly dynamically, allocated part of the memory of a processing unit of the user communications device.

When the method further comprises the step of storing the access key code in a second storage means, the access key code may be used in subsequent communications session by the first or other service communications devices.

When the second storage means is included in the second service communications device, a fast authentication may be achieved, since the access code is stored locally in the service communications devices. The second storage means may for example be a physical memory in the service communications device or a, possibly dynamically, allocated part of the memory of a processing unit of the service communications device.

Alternatively, the access key codes may be stored in a central database. In this case the access key codes may be transmitted to the individual service communications devices during an actual authentication session. It is an advantage of this embodiment that little storage capacity is required in the individual service communications devices. It is a further advantage of this embodiment that the access keys may easily be managed by a central key management system.

When the first service communications device is a designated subscription communications device, the step of generating access key codes may be localised at a small number of devices, therefore keeping the processing and memory requirements for the majority of the service communications devices simple. A designated subscription communications device may be a first point of access where the user subscribes to the service, or validates a previously received subscription, for example via a PIN code.

When the step of initiating the first communications link comprises the step of exchanging an initial access key, additional security during the initial communications session is provided.

When the step of initiating the first communications link comprises the step of transmitting a service identification code from the first service communications device to the user communications device, the service identification code may be stored in the user communications device and used for a subsequent service identification and selection of a suitable access key.

In a preferred embodiment of the invention, the step of storing the access key code in the first storage means

comprises the step of storing a service identification code.

When the step of storing the access key code in the first storage means comprises the step of storing an
5   identification code of at least one of the plurality of service communications devices, the identification code may be used in subsequent communications session, thereby increasing the security of the system.

When the method further comprises the step of using the
10   access key code to generate an encryption key, the encryption key may be used to protect the communication between the user communications device and the second service communications device, thereby providing an encryption set-up for the communication between the users
15   communications devices and the service communications devices. Consequently, it is an advantage of the invention that it provides secure communications links.

The invention further relates to a system for granting access to a service according to the method described
20   above and in the following. The system comprises a user communications device and at least one service communications device. Preferably the system is adapted to perform the authentication method described above and in the following.

25   The invention further relates to a user communications device adapted for use in a system described above and in the following.

The invention further relates to a service communications device adapted for use in a system described above and in
30   the following. The service communications device may comprise a communication unit, e.g. a Bluetooth transceiver, for communicating with the users

communications devices. The service communications device may further comprise a processing unit and a memory for storing access key codes. Furthermore, the service communications device may comprise a network interface for connecting the device with other service communications devices and/or a computer system. The service communications device may further comprise a user interface for additional user interaction and a control unit for generating a control signal based upon the results of an interaction with a user communications device.

The invention will be explained more fully below in connection with preferred embodiments and with reference to the drawings, in which:

fig. 1 shows an example of a communications system with a user communications device and three service communications devices;

fig. 2 shows a security scheme for an initial session between a mobile user communications device and a service communications device;

fig. 3 shows a security scheme for a subsequent session between a user communications device and a service communications device; and

fig. 4 illustrates an example for the use of an embodiment of the invention.

First embodiment

Introduction

The Bluetooth specifications [1] provide a set of
security features that enable Bluetooth equipped devices
5   to protect transmitted data, as well as to authenticate
other Bluetooth equipped devices upon connection to a
particular service. Here we describe a framework for the
usage of these security features in a Bluetooth Personal
Area Network with access point roaming (APR)
10   capabilities. Personal Area Networking for Bluetooth
equipped devices may be specified in a Bluetooth PAN
profile.

A Personal Area Network (PAN) can be formed with the
purpose of accessing an external network (i.e. a network
15   external to the Bluetooth PAN), through a PAN Network
Access Point (NAP). The devices providing/requesting
services set the level of security. Any device
participating in a Bluetooth PAN may demand a certain
level of security and subsequently reject a lower level
20   of security.

Bluetooth security procedures provide two mechanisms for
security, namely authentication and encryption. The
mechanisms operate on Baseband level [2]. The security
procedures are based on access to a shared secret key,
25   the passkey, between the two devices. Based on the
passkey a common access key code, the link key, is
exchanged between the devices.

Here a framework for use of the already defined Bluetooth
security procedures is described for a solution with
30   multiple Network Access Points.

Basic Bluetooth Security Protocol

A user communications device, in the following referred to as a PAN User (PANU), is able to gain access to services through a Network Access Point, e.g. internet access. The Network Access Point as well as the PANU may require a certain level of security as part of the service establishment.

Authentication and encryption is based on a bond between two Bluetooth devices. The initial step before performing authentication and encryption is to pair the two devices and establish a common link key between the two devices. Pairing is based upon the Bluetooth device address of the devices.

When a mobile node enters the NAP coverage area and detects NAP presence a part of the connection establishment procedure can be that either NAP or PANU request security procedures invoked.

Three security levels are defined:

- No security (mode 1)

- Service level requested security (mode 2)

- Security solicited by link level (mode 3)

The mentioned security modes are part of the Generic Access Profile, GAP ([3]). How they are supported in a PAN environment with support for APR is described below.

Security mode 1

Neither the mobile node nor the NAP requires security procedures invoked so this case needs no further considerations.

Security mode 2

This mode does not mandate use of any security procedures before the link setup is completed but can be invoked by the service layer. Thus it is possible to setup a connection and retrieve information about the NAP and the

5   system that the NAP is connected to.

Security mode 3

In this mode security is enforced by the link layer and requires the security procedures to be executed before link setup is completed, i.e. receiving

10   LMP_setup_complete. Thus there is an inter-dependency with regard to exchange of the BD_ADDR (Bluetooth Device Address) parameter of allowed devices. If no link key exists pairing is initiated using the common passkey which must be known and distributed to both units in

15   advance. In closed environments and systems with a limited number of access units this approach may be appropriate. In systems with multiple access points, which may be changed without notice of the mobile node, it is not feasible to use this approach.

20   Service level enforced security

Applying Bluetooth security procedures in a configuration as depicted in fig. 1 poses the challenge to support security between a PANU and multiple NAPs. Further it is possible that the NAP may be part of different logical

25   networks, i.e. macro mobility scenario. Since the PANU often has limited memory capabilities other means that the BD_ADDR information is required in order to invoke security features in a multi-NAP environment.

Applying Bluetooth security level 2 it is possible to

30   retrieve information by means of the Service Discovery Protocol (SDP) about the NAP that is being connected to. The normal NAP service record will contain information

about the security required, i.e. authentication and/or encryption. The additional information required for support of Bluetooth security in an APR environment is outlined in table 1.

Parameter	Description
Service provider identity	Unique identity of the service provider managing the system the NAP is connected to
Service provider name	Name of service provider
Logical network identity	Unique identity of network connected to
Logical network name	Name of logical network connected to
Security key support	Support for security key distribution. Values: - none - passkey - linkkey.
Higher layer security protocol	Identification of the higher layer protocols supported (WTLS, IPSec, ...)

5   Table 1, SDP service information

The information retrieval is needed in order to identify the NAP as member of a logical network handled by a known service provider; this is required in situations were more service providers are present in the same area which
10   may be the case in public hot spot areas. The PANU can in this situation use the SDP service information to

correlate against wanted service provider identity and/or logical network identity.

Basic procedure - security between unknown devices

The initial security procedures are invoked for instance in the situation that a PANU registers at a new NAP not known to the PANU; this is the basic scheme that all nodes can use.

At the initial connection towards the NAP the NAP is not recognised so pairing based upon the passkey will be initiated; the passkey must be distributed in advance and associated to the service provider identity. On the PANU this can be part of obtaining a subscription for a specific service. On the NAP this can be handled through a management system in order to distribute the passkey between all access point in the logical network.

Since the PANU may connect to any NAP in the system the BD_ADDR can not be used as identification. Using the information in the SDP record the mobile node can identify and validate if the relevant service is available. The mobile node can look up the service id in the internal DB and find the associated passkey. If no record exists the session can be terminated or continue without enabling any security.

If pairing succeeds the link key can be stored in the internal DB of the PANU and the system DB of the NAP for later use. Since the mobile node often have limited memory capabilities the mobile nodes unit key is used as link key. This way the mobile node can limit the number of link keys necessary and reuse the same link key for several relations if required (this is determined by the mobile node).

Optimised procedure

In situations where the PANU has been registered on the system and a link key has been exchanged the pairing procedure can be omitted. This can be the situation if
5 the PANU connects to a NAP of an already visited system or during a hand over between NAP's of the same system.

This scheme is proposed in order to minimise the load during hand over and reuse as much information from previous sessions as possible. Depending on the
10 information in the NAP service record authentication and/or encryption may be invoked.

The encryption function requires in addition to the link key also the cipher offset as input.
 Higher layer security

15 On top of the Bluetooth security mode the NAP is operating in, it may demand security at Ethernet layer (802.1x), IP layer (IPsec) or higher layer/application security (In case the NAP is an Ethernet bridge, it can only demand Bluetooth security and 802.1x security). This
20 can be done on per-connection base or per-service base.

Accessed services within the (fixed) network may demand additional higher layer security (e.g. IPsec or security mechanisms at transport layer or above). This can be on top of any of the above described security
25 configurations.

As a complement to distributing passkeys between nodes it is possible to use a common seed from the higher layer security protocol.

30

Service advertisement

This section describes the advertisement of security attributes for a particular PAN-based service by the Service Discovery Protocol.

5 The advertisement of a PAN service in an SDP Service Record must state the Bluetooth security requirements for accessing the service. This consists of the applicable Bluetooth security mode.

Second embodiment

10 ## Background

Bluetooth is a short-range wireless technology that enables different units to communicate with relatively high speed. Bluetooth has a large number of different applications. For many of the use cases there is a need
15 to fast set up a secure connection between two Bluetooth units. In order to exemplify the use of our invention we give a use case.

Using a Bluetooth phone for public transport ticketing

As an example, we consider the situation where a public
20 transport customer has the opportunity to subscribe to a service where he is able to use his phone as a user communications device to store and present an electronic ticket for the underground transport. The solution using Bluetooth transceivers at the underground gates as
25 service communications devices are shown in Figure 4.

Here we assume that the "pre-scanning" transceiver scan for all Bluetooth units when they are entering the underground area. Information about units approaching is then forwarded to the transceivers at the gate, which can
30 page the Bluetooth units that pass the gates and give

them access if they first are authenticated or if they can present a valid electronic ticket over the Bluetooth link. For this to work it should be possible for the transceivers at the gate to measure if a Bluetooth unit
5   is very close to the gate or more far away.

We assume that when a user for the first time physically arrives to a place where he can subscribe to a service then he subscribes to the service by connecting his Bluetooth device (e.g., phone) to the service providers
10   Bluetooth access point.

State-of-the-art

The Bluetooth baseband specification [2] describes how to create security associations between Bluetooth units, authenticate units and encrypt Bluetooth links.

15   Problem

In the use case example above as well as in other possible Bluetooth e-commerce situations there is a need to fast authenticate a Bluetooth unit or to set up a secure encrypted link between two Bluetooth units. Using
20   the Bluetooth baseband security mechanism can perform fast authentication and encryption. The Bluetooth security mechanisms are based on a shared secret link key between two Bluetooth units. There are two main types of link keys:

25   • Combination key

             • Unit key

A combination key is unique for each combination of Bluetooth units. A unit key is unique for a certain unit and this unit uses this unit key for all its connections.
30   In the applications we are considering we have a rather

large amount of different Bluetooth transceivers that we would like to connect to approaching Bluetooth units. It would be very cumbersome to demand that all the different distributed Bluetooth transceivers should share a

5 combination key with any user Bluetooth unit that has subscribed to the service. Hence, it is not feasible to use a combination key for the service we are considering. On the other hand, would it then be possible to use a unit key? Not if the unit should be able to have

10 different security levels for different links that it uses. According to the Bluetooth specification unit with unit key uses a unit key for all its connections. Furthermore, the current Bluetooth specification only describes how to create link keys when pairing two

15 devices. We can not assume that the user needs to pair his device with all possible transceivers of the service provider.

Solution

We suggest a solution with two main parts:

20 • introduce the concept of group unit keys as access key codes

• use a security infrastructure for distribution of group unit keys

We can use the current Bluetooth security mechanism with

25 very small changes if we assume that a unit key is not only used by unit with small memory capacity, but also might be used by any unit. Furthermore, we assume that a unit key is not unique for one unit but is used by one unit for one particular service, i.e., a unit might have

30 several unit keys, one for each service that it has subscribed for. This type of unit keys we called group unit key. Hence, before a unit subscribes to a service it

generates a new group unit key for that particular
service or it gets it over the from the access point
(using the current method for unit keys in the
specification). Later, when the user of the unit would
5   like to utilise the service it either manually configure
his unit which group unit key to use for all subsequent
connection or it allow this to be chosen by a higher
layer service protocol. It might be possible for the user
to enforce his unit to only use combination keys for some
10 connections while it still might allow group unit keys
for other type of connections. For example the key memory
in the unit might be like in the example in Table 2
below.

Service	BD_Address	Usage	Key
Underground X	All	User set	AB124223 23E23A12 1264BEF1 A2845D28B
Train comp A	All	User set	2343AF23 6496ECA A68BEA396 9464B47E
Any	3FA12437BC453	Always	23BD378A 93678928 AB2784BD FE376925
Any	D234BD6A24E9	Always	374585937 2691A373 12FD2839 CF381749

Table 2

15 In the table records for combination keys has the
BD_Address filled with the corresponding Bluetooth unit
address. In the example the two first keys are group unit
keys while the two second are ordinary combination keys.

The group unit key is generated when the user subscribes
20 to the service at service access points. This is only
done at one access point. After the subscription the

group unit key must be made available at all the service provider transceivers. Using any secure network connection protected by standard methods can do this, for example TLS [4] or IPsec [5]. Yet another possibility is to not distribute the key, but let the transceivers when needed connect over a network to a central database where all group unit keys and their corresponding Bluetooth addresses are stored. Of course then the database connection must be protected. Again, this can be done by any standard method (e.g. TLS, IPSec).

Merits of invention

The current invention makes it possible to use the fast Bluetooth baseband security mechanism for several Bluetooth e-commerce situations without changing the basic functionality in the Bluetooth standard.

References

[1] Bluetooth SIG, Specification of the Bluetooth system, Core, Version 1.0B, 1 December 1999, at http://www.bluetooth.com/.

[2] Bluetooth SIG, Specification of the Bluetooth system, Core, Part B "Baseband specification", Version 1.0B, 1 December 1999, at http://www.bluetooth.com/.

[3] Bluetooth SIG, Specification of the Bluetooth system, Profiles, Part K:1 "Generic Access Profile", Version 1.0B, 1 December 1999, at http://www.bluetooth.com/

[4] T. Dierks and C. Allen, "The TLS Protocol Version 1.0", IETF RFC 2246, ftp://ftp.isi.edu/in-notes/rfc2246.txt

[5] Atkinsson. R., "Security Architecture for the Internet Protocol", IETF RFC 2401, ftp://ftp.isi.edu/in-notes/rfc2401.txt

Glossary

5   Network Access Point (NAP): The service communications device providing access to a network, e.g. LAN Access Point.

PAN User (PANU): The user communications device that uses the services of a Network Access Point.

CLAIMS

1. A method of granting, to a user communications device, access to a plurality of service communications devices providing a service, the method comprising the steps of

5   initiating a first communications link between the user communications device and a first one of the plurality of service communications devices;

creating an access key code indicative of the user communications device and the service;

10   storing the access key code in a first storage means of the user communications device;

transmitting the access key code from the first service communications device to at least a second one of the plurality of service communications devices;

15   initiating a second communications link between the user communications device and the second service communications device; and

using the access key code to mutually authenticate the user communications device and the second service
20   communications device.

2. A method according to claim 1, characterised in that a selected one of the first and second communications links is a Bluetooth communications link.

3. A method according to any one of the claims 1 through
25   2, characterised in that the user communications device is a mobile station.

4. A method according to any one of the claims 1 through 3, characterised in that the method further comprises the

step of storing the access key code in a second storage means.

5. A method according to any one of the claims 1 through 4, characterised in that the second storage means is included in the second service communications device.

6. A method according to any one of the claims 1 through 5, characterised in that the step of transmitting the access key code comprises the step of transmitting the access key code via a secure network connection.

7. A method according to any one of the claims 1 through 6, characterised in that the first service communications device is a designated subscription communications device.

8. A method according to any one of the claims 1 through 7, characterised in that the step of initiating the first communications link comprises the step of exchanging an initial access key.
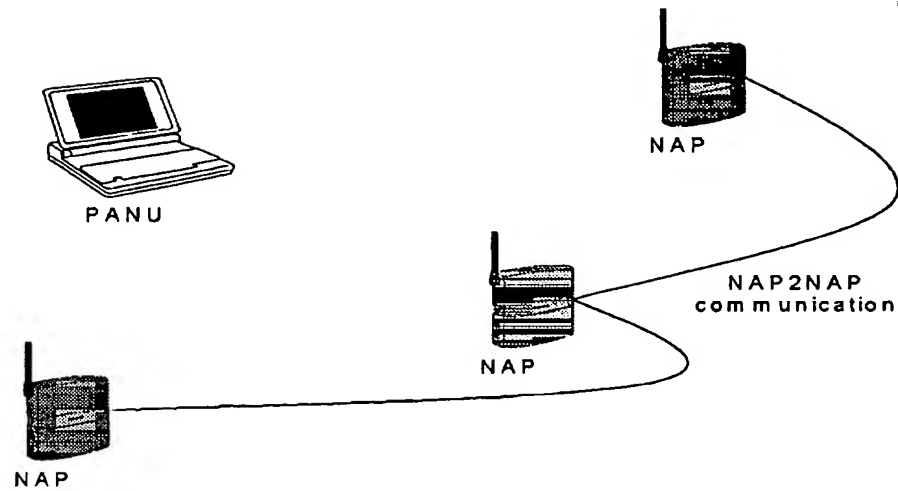
9. A method according to any one of the claims 1 through 8, characterised in that the step of initiating the first communications link comprises the step of transmitting a service identification code from the first service communications device to the user communications device.

10. A method according to any one of the claims 1 through 9, characterised in that the step of storing the access key code in the first storage means comprises the step of storing a service identification code.
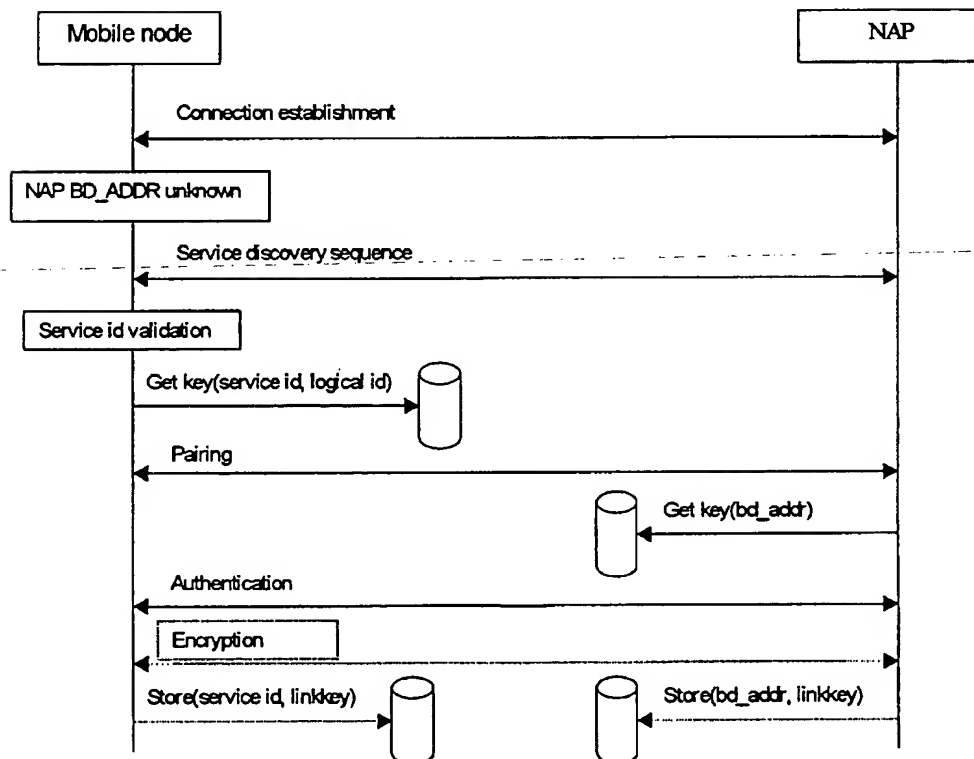
11. A method according to any one of the claims 1 through 10, characterised in that the step of storing the access key code in the first storage means comprises the step of storing an identification code of at least one of the plurality of service communications devices.

12. A method according to any one of the claims 1 through 11, characterised in that the method further comprises the step of using the access key code to generate an encryption key.
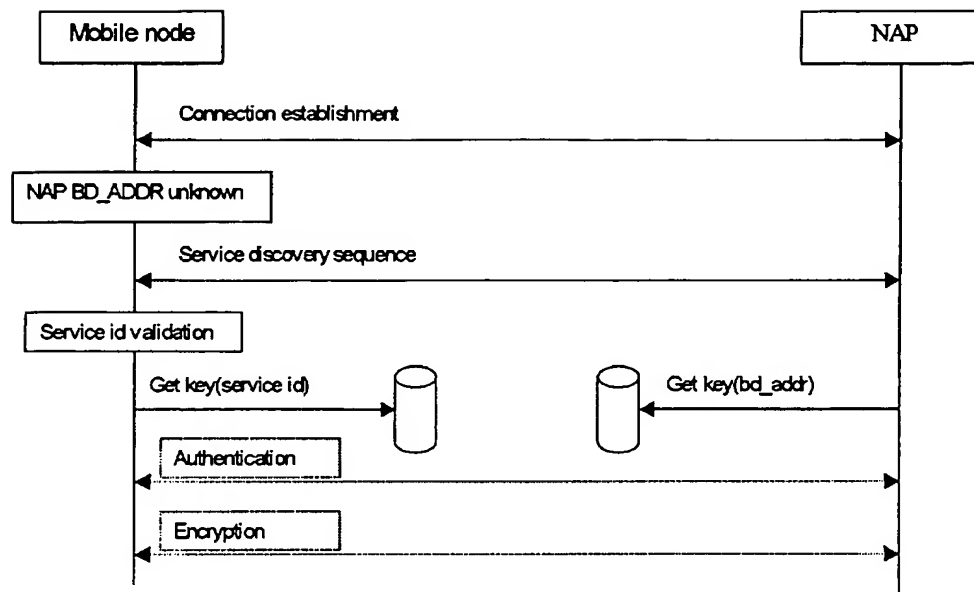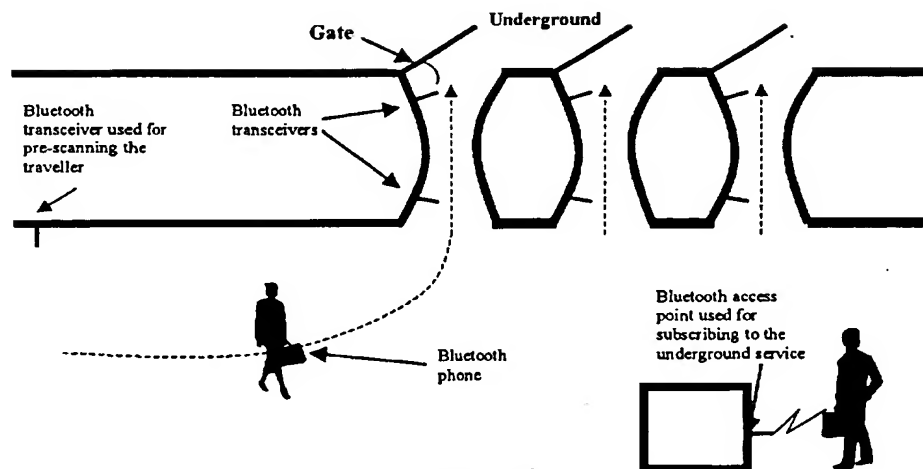
5

NAP

PANU

NAP

NAP2NAP
communication

NAP

Fig. 1

Mobile node		NAP

Connection establishment

NAP BD_ADDR unknown

Service discovery sequence

Service id validation

Get key(service id, logical id)

Pairing

Get key(bd_addr)

Authentication

Encryption

Store(service id, linkkey)   Store(bd_addr, linkkey)

Fig. 2

Fig. 3

Fig. 4